47

cuales se accedió a la misma, limitándose a indicar que la cuenta había sido creada el 23 de julio de 2019, a nombre de Superintendencia de Bienestar, y que registraba como país de creación los Estados Unidos (fs. 1602)

En ese sentido se advierte que entre el inicio del expediente (fs. 1) y la decisión judicial de requerir la información (fs. 42) pasaron unos 14 días en los cuales puede haberse perdido valiosa información.

Si bien es cierto que durante ese tiempo el caso pasó por al menos tres jueces (el que estaba de turno con la dependencia policial que inició las actuaciones hasta el momento de su sorteo, la que pasó a intervenir luego del sorteo y quien en definitiva se quedó a cargo por declinación de competencia) los investigadores originarios podrían, desde un primer momento, haber preservado los registros de las cuentas (art. 16 Convenio sobre la Ciberdelincuencia) como es de estilo para evitar que la volátil evidencia electrónica se pierda[10].

2.2. Servidores accedidos ilegítimamente.

Se recolectó la información resguardada en los servidores con relación al sitio web engañoso, y se constató que las credenciales provistas por las víctimas eran resguardadas en un archivo de texto identificado como "log.txt" (fs. 32 y siguientes del legajo). En el documento se encontraron diversas direcciones de email asociadas a contraseñas y direcciones IP, hallándose mencionada entre éstas la casilla areaoctava.mesopotamia@gmail.com. A su vez, se relevó la información de las conexiones registradas por el *firewall.*

Dadas las particularidades del caso, se consideró que la página en cuestión pudo haber sido montada mediante técnicas de inyección de código PHP.

Se analizó otro de los archivos obtenidos en el marco de las referidas labores, identificado como "error.log" -respecto al cual no se indicó si correspondía a los registros del firewall, del servidor o de qué servicio-, en el que se constató que el 10 de agosto de 2019, desde la dirección IP 199.58.[redacted], correspondiente al proveedor de servicios de internet Full Tech Solutions S.H (con sede en Villa Elisa, provincia de Entre Ríos), se había accedido o intentado acceder a diferentes rutas dentro del servidor (fs.708 del legajo).

Huelga decir que las circunstancias que rodearon el montaje de un sitio de *phishing* (captación engañosa de datos) dentro de una web oficial deberían analizarse exhaustivamente no sólo para deslindar responsabilidades sino también para que a futuro estas situaciones no se repitan. Otro tanto respecto de la cuestionable, desde varios puntos de vista, utilización de cuentas de correo no oficiales por parte de agencias policiales, la falta de adopción de medidas de seguridad que hubiesen minimizado los riesgos (como activar la

[10] Ver, entre otros documentos, párrafo 155 del reporte explicativo al Convenio sobre la Ciberdelincuencia. Versión en español en https://rm.coe.int/16802fa403 y, en inglés, UNODC - Practical Guide for Requesting Electronic Evidence Across Borders https://www.unodc.org/unodc/en/frontpage/2019/January/unodc-and-partners-release-practical-guide-for-requesting-electronic-evidence-across-boarders.html